

FILED

MAR 22 2016

MAGISTRATE JUDGE, JEFFREY COLE
UNITED STATES DISTRICT COURT

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case Number:

The Facebook account antonio.dunner.5, further
described in Attachment A

16M146

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, David I. Young, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of California, there is now concealed:

See Attachment A, Part III

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities.

The search is related to a violation of:

Code Section

Offense Description

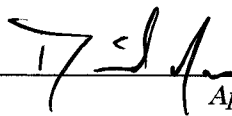
Title 18, United States Code, Section 1951(a)

conspiracy to commit Hobbs Act robbery

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.



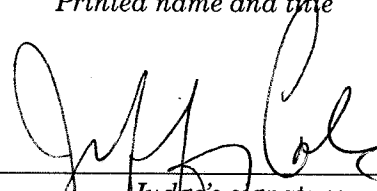
Applicant's Signature

DAVID I. YOUNG, Special Agent, Federal Bureau of
Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: March 22, 2016



Judge's signature

City and State: Chicago, Illinois

JEFFREY COLE, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, DAVID I. YOUNG, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed for approximately 16 years.

2. I am currently assigned to the FBI's North Resident Agency, and my responsibilities include the investigation of violent crimes, including kidnapping, robbery, and the apprehension of violent fugitives. I have participated in the investigation of multiple robberies and the execution of multiple federal search warrants.

3. This affidavit is made in support of an application for a warrant to search, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain accounts that are stored at the premises owned, maintained, controlled, or operated by Facebook, a social network provider located at 1601 S. California Avenue, Palo Alto, California 94304. The account to be searched is antonio.dunner.5 (hereinafter, "**Subject Account 1**"), which is further described in the following paragraphs and in Part II of Attachment A. As set forth below, there is probable cause to believe that in **Subject Account 1**, in the possession of Facebook, there exists evidence of a violation of Title 18, United States Code, Section 1951(a).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because I am submitting this affidavit for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of a violation of Title 18, United States Code, Section 1951(a), are located in **Subject Account 1**.

BACKGROUND INFORMATION

Facebook

5. Based on my training and experience, I have learned the following about Facebook:

a. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, email addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites,

and other personal identifiers. Facebook also assigns a user identification number to each account.

c. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

d. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos,

photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

f. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to “tag” (*i.e.*, label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

g. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

h. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

i. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

j. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

k. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

l. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification

numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

m. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

n. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

6. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Facebook, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Facebook to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

**FACTS SUPPORTING PROBABLE CAUSE TO SEARCH SUBJECT
ACCOUNT 1**

7. The FBI and local law enforcement have been investigating a series of armed robberies that occurred at ATMs in the following locations and times, which are related:

- a. On or about 10:20 p.m., on August 19, 2015, at the Chase Bank located at 1600 Larkin Avenue, Elgin, Illinois;
- b. On or about 10:58 p.m., on September 12, 2015, at the Chase Bank located at 21 South Western Avenue, Carpentersville, Illinois;

c. On or about 10:09 p.m., on September 16, 2015, at the Chase Bank located at 727 Roosevelt Road, Glen Ellyn, Illinois;

d. On or about 9:37 p.m., on September 23, 2015, at the Chase Bank located at 2801 Dundee Road, Northbrook, Illinois;

e. On or about 11:06 p.m., on September 23, 2015, at the Chase Bank located at 500 Busse Highway, Park Ridge, Illinois;

f. On or about 10:13 p.m., on September 28, 2015, at the Chase Bank located at 43 East Golf Road, Arlington Heights, Illinois;

g. On or about 11:35 p.m., on October 8, 2015, at the Chase Bank located at 4200 Dundee Road, Northbrook, Illinois; and

h. On or about 9:45 p.m., on October 19, 2015, at the Chase Bank located at 43 East Golf Road, Arlington Heights, Illinois.

8. The victims in each of the robberies described the robbers as being one or two black males approximately late teens to early twenties, wearing dark hooded sweatshirts covering their heads, bandanas covering their faces, carrying a black handgun, and in some cases wearing gloves and dark pants.

9. Additionally, based on review of surveillance footage, during the October 8, 2015 robbery, one of the robbers was wearing a black hoodie that had the word "redbirds" written on the side of the hood in red lettering. Likewise, the victim in the October 19 robbery reported that one of the robbers wore a dark hoodie with red and white lettering on it.

10. On October 9, 2015, Chief Judge Ruben Castillo, upon application of the government, issued an order directing disclosure of cell tower information related to the cell phone numbers that were activated near the robberies that took place between August 19, 2015, and October 8, 2015,¹ around the times of the robberies. After receiving the information, law enforcement's analysis of the data revealed that cell phone number 224-829-5988 ("CD 1's Phone") was used in the vicinity of six of the robbery locations during the forty minutes before or twenty minutes after those robberies.

11. Based on the information obtained regarding CD 1's Phone, on October 30, 2015, upon application of the government, Chief Judge Ruben Castillo issued an order directing disclosure of information related to CD 1's Phone, including real-time monitoring of CD 1's Phone's location. From October 30, 2015, through November 2, 2015, law enforcement received GPS location data for CD 1's Phone.

12. According to location data obtained pursuant to the October 30, 2015 order, on or about November 1, 2015, CD 1's Phone was in the vicinity of a Shell gas station, located at 301 W. Butterfield Road, Elmhurst, Illinois, at around the time this gas station was robbed. According to the victim who is a Shell employee, after the victim finished his closing duties and unlocked the front doors of the Shell to

¹ The remainder of the robberies had not yet taken place. In addition, because the September 16, 2015 robbery was inadvertently listed as having taken place on September 18, 2015, law enforcement did not receive cell tower data related to the September 16th robbery.

exit the building and leave for the night around approximately 10:50 p.m., two unknown black males (the "robbers") were wearing dark jackets, dark hoodies, dark pants, and masks approached the victim. One of the robbers was holding a handgun and ordered the victim back into the store. The robber with the gun said words to the effect of, "Where is the money?" Inside the store, the robbers forced the victim to open the cash register, from which the robbers took approximately \$350 before leaving the store. The victim described the first robber as a black male, approximately 6' tall and skinny, wearing a black jacket, black pants, and a mask. The victim described the second robber as a few inches shorter than the first robber, wearing the same clothes and a similar mask to the first robber. The surveillance footage shows that one of the robbers was wearing, amongst other clothing, a black hooded sweatshirt that had red lettering on the side of the hood.

13. Approximately two hours after the Shell gas station robbery, law enforcement arrested an individual, Cooperating Defendant (CD) 1, in Carpentersville, Illinois, following a traffic stop during which CD 1 admitted to having just smoked marijuana.

14. Carpentersville Police Department (CPD) officers conducted an inventory search on the vehicle prior to it being towed and impounded. During the inventory search, CPD officers found a black hooded sweatshirt with an Illinois State University logo on the front and the word "Redbirds" written down the side of the hood in red lettering in the passenger compartment.

15. According to CPD officers, when CD 1 was booked after his arrest, he told CPD officers that his cellphone number was 224-829-XXX, which is the phone number associated with CD 1's Phone. A CPD officer called the 224-829-XXX number to confirm that the phone in CD 1's possession corresponded to the telephone number that CD 1 provided and the phone rang and showed the CPD officer's number.

16. Law enforcement reviewed the GPS location data for CD 1's Phone that law enforcement obtained pursuant to the Court's October 30, 2015 order. The data showed that CD 1's Phone was in the vicinity of the Shell gas station around the time of the robbery on November 1, 2015. More specifically, the Shell gas station was robbed at approximately 10:50 p.m., and GPS information shows that CD 1's Phone was located in the vicinity of the Shell gas station at 10:17 p.m., 10:33 p.m., and 10:49 p.m. on the date of the robbery.

17. On or about November 3, 2015, CD 1 was arrested and charged by federal complaint in connection with the November 1, 2015 robbery of the Shell gas station.

18. Following his arrest, CD 1 participated in several interviews with the government.² During these interviews, CD 1 admitted to committing the eight robberies listed in Paragraph 7 as well as the November 1, 2015 robbery of the Shell

² CD 1 met with the government and provided information in the hopes of receiving a reduced sentence or charging consideration in connection with his pending case. The government has not made any promises to CD 1.

gas station. CD 1 told law enforcement that he committed the September 16 and 23, October 8 and 19, and November 1, 2015 robberies with an individual named ANTONIO DUNNER. According to CD 1, he and DUNNER are good friends. After DUNNER learned that CD 1 had committed the August 19 and September 12 robberies, DUNNER asked to be involved in future robberies and CD 1 agreed. CD 1 stated that he drove himself and DUNNER to the robberies and that he and DUNNER split the robbery proceeds 50-50. CD 1 further stated that DUNNER's phone number was listed in CD 1's cell phone under the name AO Streak, which is DUNNER's nickname. Law enforcement obtained a search warrant for CD 1's phone and found that the phone number listed under AO Streak in CD 1's Phone is 224-595-XXXX ("DUNNER's Phone").

19. Subsequent investigation corroborates CD 1's information. Video surveillance confirms that there were two robbers present at the September 16 and 23, October 8 and 19, and November 1, 2015 robberies.

20. DUNNER is a black male who is approximately 6'0" tall, which is generally consistent with the victims' descriptions of the robbers.

21. Further, law enforcement located a Facebook profile under the name Antonio Dunner, **Subject Account 1**. Law enforcement identified the profile as DUNNER's based on the profile picture in the Facebook profile. The publicly available part of **Subject Account 1** lists DUNNER's Phone as his phone number. In addition, the publicly available part of **Subject Account 1** contains a link to rap

videos by "AO \$treaks." DUNNER is the primary rapper in the videos. Law enforcement identified DUNNER based on review of known photographs of DUNNER.

22. Text message evidence corroborates DUNNER's involvement in the robberies. During the search of CD 1's Phone, law enforcement identified text messages from some of the dates of the robberies. On November 1, 2015, for example, the date of the Shell robbery, the following text messages, amongst others, were exchanged between CD 1's Phone and DUNNER's Phone:

DUNNER at 12:36 p.m.: "What time you thinking bout riding out?"

CD 1 at 12:36 p.m.: "Like 8:30 9"

CD 1 at 8:14 p.m.: "On my way"

DUNNER at 8:21 p.m. "Iight I'm on my waya to the crib from the east"

CD 1 at 8:39 p.m.: "Iight I'm outside"

DUNNER at 8:40 p.m.: "Iight I'm bout to pull up and run in real quick"

23. As noted above, the Shell robbery occurred approximately two hours after these text messages were sent. According to CD 1, DUNNER and CD 1 were discussing meeting to go to rob the Shell station in this series of text messages.

24. CD 1 also told law enforcement that he occasionally texted DUNNER regarding robberies. For example on or about October 8, 2015, CD 1 and DUNNER had the follow exchange via text message:

CD 1 at 2:10 p.m.: "On me I found 3 more locations today they all low key"

DUNNER at 2:24 p.m.: "G let's hit at least 2 man. We need it all!"

CD 1 at 2:26 p.m.: "On me bro"

25. As noted above, the Chase Bank located at 4200 Dundee Road, Northbrook, Illinois was robbed the evening of October 8, 2015. According to CD 1, DUNNER and CD 1 were discussing additional Chase ATM locations at which they could rob people.

26. Cell site data further corroborates DUNNER's involvement in the robberies. On or about December 7, 2015, upon application of the government, Chief Judge Ruben Castillo issued order directing disclosure of DUNNER's historical cell site data. Analysis of DUNNER's historical cell site data, revealed that DUNNER was in the vicinity of all of the ATM robberies that CD 1 alleged that DUNNER participated in.³ On September 16, 2015, DUNNER's Phone activated a cell tower that was approximately .3 miles away from the robbery location approximately 30 minutes before the robbery. On September 23, 2015, DUNNER's Phone activated a cell tower that was approximately 11.1 miles away from the first robbery location approximately 35 minutes before the robbery, and approximately .4 miles away

³ Cellular service providers maintain antenna towers ("cell towers") that serve specific geographic areas. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. These cell towers allow the wireless devices to transmit or receive communications, such as phone calls, text messages, and other data. The tower closest to a wireless device does not necessarily serve every call made to or from that device. Cell site data thus is not as precise as GPS data, but it can provide reliable information about the general location of a phone at the time it is used.

from the second robbery location approximately 15 minutes before the robbery. On October 8, 2015, DUNNER's Phone activated a cell tower that was .2 miles away from the robbery approximately four minutes before the robbery. On October 19, 2015, DUNNER's Phone activated a cell tower that was 1.3 miles away from the robbery approximately 25 minutes before the robbery. On November 1, 2015, the date of the robbery of the Shell gas station, DUNNER's Phone activated a cell tower that was approximately 2.5 miles away from the robbery approximately an hour before the robbery.

27. DUNNER's residence is located in Elgin, Illinois, which is approximately 18 to 31 miles away from the locations of the robberies that DUNNER committed.

28. On or about March 8, 2016, DUNNER was charged by complaint with conspiracy to commit Hobbs Act robbery (16 CR 158).

Relevance of Subject Account 1

29. During the course of this investigation, agents learned that CD 1's girlfriend, Individual A, communicated with DUNNER through private messages sent to **Subject Account 1**. According to Individual A, CD 1 contacted her via telephone shortly after CD 1 was arrested in November 2015. CD 1 told Individual A to tell DUNNER that CD 1 was in federal jail. Individual A located DUNNER on Facebook and communicated with DUNNER via **Subject Account 1** regarding CD 1's arrest. Individual A also arranged via **Subject Account 1** a meeting between

DUNNER and Individual B, CD 1's stepfather, so that the DUNNER and Individual B could discuss CD 1's arrest.

30. In addition, as discussed above in paragraph 21, the publicly available part of **Subject Account 1** lists DUNNER's Phone as his phone number. The publicly available part of **Subject Account 1** also contained a link to rap videos by "AO \$treaks," which is a nickname used by DUNNER.

31. Based on my training and experience in other investigations, I believe that a search of social network provider account contents of individuals engaged in criminal conduct often yields investigative leads relating to:

- a. the identities of co-conspirators and other individuals engaged in the conspiracy;
- b. the contact information of co-conspirators and other individuals engaged in the conspiracy;
- c. the planning of the conspiracy; and
- d. the methods and techniques used in committing the conspiracy.

32. In this instance, there is evidence that DUNNER used **Subject Account 1** to communicate about the robberies. Because these communications are not publicly visible, the requested search warrant is necessary to obtain the private messages sent to or from **Subject Account 1**. In addition, there is evidence that information in **Subject Account 1** connects DUNNER to the robberies, including, amongst other things, DUNNER's contact information and information regarding

nicknames used by DUNNER. Therefore, the requested search warrant is likely to lead to relevant evidence of the robberies under investigation.

SEARCH PROCEDURE

33. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Facebook to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Facebook personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Facebook employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II of Attachment A, including an exact duplicate of all information described in Section II of Attachment A;

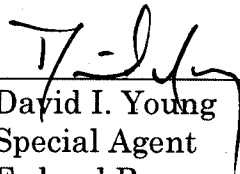
c. Facebook employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

d. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from Facebook employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

CONCLUSION

34. Based on the above information, I respectfully submit that there is probable cause to believe that evidence and instrumentalities of a violation of Title 18, United States Code, Section 1951(a) are located within one or more computers and/or servers found at Facebook, headquartered at 1601 S. California Avenue, Palo Alto, California 94304. By this affidavit and application, I request that the Court issue a search warrant directed to Facebook allowing agents to seize the electronic evidence and other information stored on the Facebook servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.



David I. Young
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 22nd day of March, 2016



Honorable JEFFREY COLE
United States Magistrate Judge

ATTACHMENT A

I. Search Procedure

1. The search warrant will be presented to Facebook personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Facebook employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Facebook Employees

To the extent that the information described below in Section III is within the possession, custody, or control of Facebook, headquartered at 1601 S. California Avenue, Palo Alto, California 94304, Facebook is required to disclose the following information to the government for the user ID: antonio.dunner.5.

(a) All contact information for antonio.dunner.5, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All Photoprints, including all photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them.

(c) All Neoprints, including profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

(d) All other communications and messages made or received by the user, including all private messages and pending "Friend" requests.

(e) All IP logs, including all records of the IP addresses that logged into the account.

(f) All information about the user's access and use of Facebook Marketplace.

(g) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number).

(h) All privacy settings and other account settings.

(i) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities concerning a violation of Title 18, United States Code, Section 1951(a), as follows:

(1) Communications to and from **Subject Account 1** regarding robberies or the use of firearms to conduct robberies;

(2) Photographs, images, collages, and videos related to robberies or the use of firearms in connection with robberies;

(3) Records reflecting the identity of any other individuals that may have been working with DUNNER to commit robberies;

(4) All transactional information of all activity of the electronic mail addresses and/or individuals associated with **Subject Account 1**, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

(5) All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses, and/or individual accounts associated with **Subject Account 1**, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

(6) All contact information for **Subject Account 1**, including full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers, and for group ids, a list of users currently registered to the group and information about the group head or administrator;

(7) All IP logs for **Subject Account 1**;

(8) All records pertaining to communications between Facebook and any person regarding **Subject Account 1**, including contacts with support services and records of actions taken;

(9) Communications to and from **Subject Account 1** and Individual A or CD 1;

(10) Communications discussing any meeting or communication between Individual B and DUNNER; and

(11) All items related to the name "AO Streak" or "AO \$treak."

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the social network provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.
- b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.
- c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or
- d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case Number:

16M146

The Facebook account antonio.dunner.5, further
described in Attachment A

SEARCH AND SEIZURE WARRANT

To: David I. Young and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of
the following person or property located in the Northern District of California:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the
person or property described above, and that such search will reveal:

See Attachment A, Part III

YOU ARE HEREBY COMMANDED to execute this warrant on or before April 6, 2016 in the daytime
(6:00 a.m. to 10:00 p.m.).

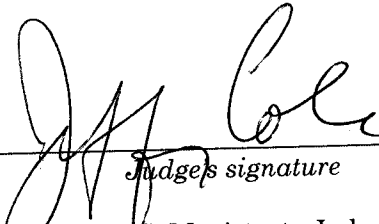
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at
the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare
an inventory as required by law and promptly return this warrant and inventory to the issuing United States
Magistrate Judge.

Date and time issued: March 22, 2016

City and State: Chicago, Illinois

9:30 Am


Judge's signature

JEFFREY COLE, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No:

Date and Time Warrant Executed:

Copy of Warrant and Inventory Left With:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

I. Search Procedure

1. The search warrant will be presented to Facebook personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Facebook employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Facebook Employees

To the extent that the information described below in Section III is within the possession, custody, or control of Facebook, headquartered at 1601 S. California Avenue, Palo Alto, California 94304, Facebook is required to disclose the following information to the government for the user ID: antonio.dunner.5.

(a) All contact information for antonio.dunner.5, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All Photoprints, including all photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them.

(c) All Neoprints, including profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

(d) All other communications and messages made or received by the user, including all private messages and pending "Friend" requests.

(e) All IP logs, including all records of the IP addresses that logged into the account.

(f) All information about the user's access and use of Facebook Marketplace.

(g) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number).

(h) All privacy settings and other account settings.

(i) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities concerning a violation of Title 18, United States Code, Section 1951(a), as follows:

(1) Communications to and from **Subject Account 1** regarding robberies or the use of firearms to conduct robberies;

(2) Photographs, images, collages, and videos related to robberies or the use of firearms in connection with robberies;

(3) Records reflecting the identity of any other individuals that may have been working with DUNNER to commit robberies;

(4) All transactional information of all activity of the electronic mail addresses and/or individuals associated with **Subject Account 1**, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

(5) All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses, and/or individual accounts associated with **Subject Account 1**, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

(6) All contact information for **Subject Account 1**, including full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers, and for group ids, a list of users currently registered to the group and information about the group head or administrator;

(7) All IP logs for **Subject Account 1**;

(8) All records pertaining to communications between Facebook and any person regarding **Subject Account 1**, including contacts with support services and records of actions taken;

(9) Communications to and from **Subject Account 1** and Individual A or CD 1;

(10) Communications discussing any meeting or communication between Individual B and DUNNER; and

(11) All items related to the name "AO Streak" or "AO \$treak."

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the social network provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.